(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75900 A1

(51) International Patent Classification⁷: G08B 25/14, 26/00, 25/10, 25/08

(21) International Application Number: PCT/CA00/00662

(22) International Filing Date: 6 June 2000 (06.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,274,572 7 June 1999 (07.06.1999) CA

(71) Applicant *(for all designated States except US)*: STRATEGIC VISTA INTERNATIONAL INC. [CA/CA]; 300 Alden Road, Markham, Ontario L3R 4C1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: KLIGMAN, Joel [CA/CA]; 15 Invermay Avenue, Toronto, Ontario M3H 1Z1 (CA). KLEIN, Bernie [CA/CA]; 190 Bedford Road, Toronto, Ontario M5R 2K9 (CA).

(74) Agents: EISEN, Mark, B. et al.; Dimock Stratton Clarizio, Suite 3202, 20 Queen St. West, Box 102, Toronto, Ontario M5H 3R3 (CA).

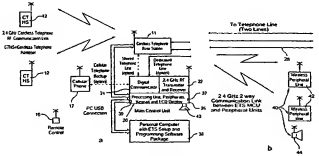
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) Title: PROGRAMMABLE SECURITY ALARM SYSTEM



(57) Abstract: A wireless security alarm system providing reliable two-way communication between a control unit and a plurality of peripheral devices, including sensors, alarm indicators and remote controls. The system of the invention provides a large number of channels for monitoring both intrusion and environmental conditions, and can include emergency dialing capabilities for the elderly or small children. A monitoring service can monitor the premises, and upon detecting an alarm condition to process audio and/or video data allowing the monitoring service to watch and/or listen to events occuring within the premises and dispatch an appropriate emergency response, and to communicate with persons within the premises during an emergency. The peripherals used in system of the invention can be configured through the control unit and automatically or remotely reconfigured if the control unit detects attempts to tamper with peripherals or jam the signals to the control unit. The system may be programmed by connection to a local or remote personal computer. To reduce the incidence of false alarms in response to an indication of an alarm condition by a sensor the main control unit may request a status signal from the sensor, and/or from one or more neighboring sensors, to verify the alarm condition. A cordless telephone handset may function as a remote control device for the system, wherein an LCD displays system status and other desired indicators, and the telephone keypad is used for data entry and activation or deactivation of the alarm system. A cellular, pager or two-way radio connection backup may be provided in case of sabotage or failure of the telephone line, or used as the primary communications line.

WO 00/75900 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PROGRAMMABLE SECURITY ALARM SYSTEM

Field of Invention

This invention relates to security alarm systems. In particular, this invention relates to a programmable security alarm system providing reliable two-way communication between a main control unit and a plurality of peripheral devices.

Background of the Invention

Security alarm systems are used in homes and in commercial and industrial facilities, for monitoring the premises to detect intruders, fire and environmental hazards such as carbon monoxide contamination. There are two types of security alarm systems: wired and wireless. Although both have been proven effective over many years, security alarm systems are still utilized in a minority of premises because of the cost and limitations of conventional systems.

Much of the cost of installing a wired alarm system is in the installation of the wiring, since the peripheral devices such as sensors (typically contact, motion detectors and vibration detectors) and alarm condition indicators (such as sirens, bells and telephone line seizing devices in the case of monitored systems) are dispersed throughout the premises and thus well remote from the control unit. In general it is advantageous to divide the premises into "zones" which are monitored independently, and although the sensors within a zone can be wired in series the zone circuits must be connected to the control unit in parallel in order for the control unit to be able to discriminate between zones.

A lot of wiring is required to adequately cover vulnerable entry points divided into a desirable number of zones, and a service technician installing such a system must thus spend considerable time fishing wires through walls in order to make the alarm system unobtrusive. This is a time consuming and costly procedure, and it is not always possible to conceal the wiring in structures such as condominiums and apartment buildings, older houses and houses with finished basements.

Wireless alarm systems are also known. In these systems a plurality of different kinds of sensors distributed about the premises each emit a radio frequency (RF) signal with a

characteristic frequency. The signal is transmitted when the sensor detects an intrusion, for example a point contact which is broken when a window is forced open or a motion detector which senses motion within its detection field. A receiver contained in a control unit monitors the various RF signals and signals a control unit when one or more of these signals is transmitted, indicating an alarm condition.

Wireless alarm systems are considerably easier to install, because peripheral sensors need only be mounted and do not have to be wired to the control unit. However, in a typical wireless system there are a limited number of RF channels available for peripheral sensors, and the cost of the system increases considerably as more channels are added.

Further, these systems provide only one-way communication, i.e. sensor-to-base signals, and thus alarm indication peripherals such as audible indicators and line seizing devices must still be wired to the control unit, which increases installation costs. In some cases the RF signals emitted by the sensors have a limited range before they become subject to interference and unreliability, which can limit the location of such peripherals and/or the control unit itself. Also, the one-way communication of such systems precludes any verification procedure, which can result in false alarms caused by equipment malfunction and lead to costly and unnecessary response by emergency services personnel.

Moreover, the versatility of both wired and wireless alarm systems is in part determined by the capacity to set and change parameters of the system. However, with increased programming capability arises the requirement for a more complex programming interface. This increases the size, complexity and cost of the alarm system. This also increases the complexity of installation, since the limited display window typically incorporated into such devices permits only small amounts of information to be displayed to the installer at any particular time; thus, in a complex system offering many programmable features the installer must be trained to be fully familiar with all of the programming functions and procedures of the device, or is constrained to review extensive operating instructions, in order to properly utilize the more complex features of the system. Accordingly, manufacturers often compromise on the versatility of the alarm system by omitting potentially advantageous features in order to avoid the need to increase the cost and complexity of the programming interface.

Summary of the Invention

The present invention overcomes these problems by providing a wireless security alarm system providing reliable two-way communication between a control unit and a plurality of peripheral devices, including both sensors and alarm indicators. In the preferred embodiment the control unit of the invention operates in conjunction with a cordless telephone, providing instantaneous access to a telephone line for monitoring by a security service or auto-dialing to an emergency number, and allowing the telephone handset to be used as a remote control and user display for setting alarm functions after installation.

In the preferred embodiment the control unit incorporates an interface for a digital processing device such as a personal computer. This allows the control unit to be programmed to perform a variety of functions using programming software that provides an extensive user interface, thus allowing the alarm system to be extremely versatile while considerably simplifying the installation and setup operations. The ability to connect the system to a computer also provides comprehensive diagnostic capabilities for testing, maintenance and repair of the system, and connection to computer networks, including the Internet.

The system of the invention can accordingly be easily installed by a home or business owner without any special tools and requires no wiring through the premises. The system of the invention provides a large number of channels for monitoring and response to both intrusion and environmental conditions, and can include emergency dialing capabilities for the elderly or small children, and a variety of home automation capabilities (HVAC, etc.).

The alarm system of the invention allows a monitoring service to monitor the premises, and upon detecting an alarm condition to process audio and/or video data allowing a monitoring service to watch and/or listen to events occurring within the premises and dispatch an appropriate emergency response, and to communicate with persons within the premises during an emergency. The peripherals used in system of the invention can be configured through the control unit upon installation, either directly or from a remote location, and automatically or remotely reconfigured if the control unit detects attempts to tamper with peripherals or jam the signals to the control unit; to initiate or discontinue a battery-saving "sleep" mode; and/or to adjust environmental controls or preprogrammed

procedures. The auto-dial feature can also be configured remotely, allowing a user to remotely select one or more of a plurality of stored telephone numbers for the emergency dialer.

In the preferred embodiment this is accomplished by providing the control unit with a built-in digital communicator having full upload and download capabilities, permitting remote programming, alarm reception and verification and analysis of an alarm condition. Where the system is implemented in conjunction with a cordless telephone, an LCD display on the telephone handset displays system status and other desired indicators, and the telephone keypad can be used for data entry and activation or deactivation of the alarm system (optionally with a separate key fob remote control).

The control unit memory may be adapted to store any desired number of alarm events in an event log. This information can be downloaded to the personal computer periodically, to maintain ongoing records relating to the security of the premises.

Utilizing a bi-directional digital communication data link, preferably in the 2.4 GHz frequency range, the alarm system of the invention easily accommodates many different channels each with a unique signal ID code, allowing many more peripherals and zone configurations than a conventional wireless alarm system of comparable cost. The signals are reliable over a large distance, in most environments up to or over 100 meters, permitting integration of alarm systems in different premises of a residential or commercial complex or structure. Where the communications protocol operates in the 2.4 GHz range (or other frequencies with sufficiently wide bandwidth), the system allows for high speed transfer of video and other data, for example from surveillance cameras installed in and around the secured premises.

In the preferred embodiment the system of the invention provides a cellular or two-way radio connection, either as the primary communications line or as a backup in case of sabotage or failure of the telephone line, and a self-testing function for monitoring such events. Optionally connection with the system via two-way pager is provided as a further backup measure and/or for direct user response to an alarm condition. The invention can be applied to all conventional intrusion detection peripherals, including glass breakage sensors, and also to environmental monitoring such as smoke and fire detection, hazardous gas

detection, temperature, water and/ or moisture detection, etc. Connection to a local or remote personal computer is also available for expanded operation, detailed system analysis and/or integration with other systems.

The present invention thus provides a security alarm system, comprising one or more peripheral units, and a main control unit comprising an RF transceiver for communicating with the one or more peripheral units, whereby the main control unit receives a signal from the one or more peripheral units to indicate an alarm condition, and a digital communications port, wherein the main control unit can be connected to a digital processing device through the digital communications port, whereby data entered into the digital processing device programs the main control unit.

The present invention further provides a method of programming a security alarm system comprising one or more peripheral units, and a main control unit comprising an RF transceiver for communicating with the one or more peripheral units, whereby the main control unit receives data from the one or more peripheral units to indicate an alarm condition, and a digital communications port, comprising the steps of a. connecting the main control unit to a digital processing device through the digital communications port, and b. entering data into the digital processing device to program the main control unit.

In further aspects of the invention the main control unit communicates data to the one or more peripheral devices to configure and control said peripheral devices; the main control unit comprises a communicator for controlling a transfer of data between the system and a remote location over a communications link; a keypad or a display, or both, are contained in a remote unit, which may be a cordless telephone handset and/or a key chain; in response to an indication of an alarm condition by a sensor, the main control unit requests a status signal from the sensor and/or from one or more neighboring sensors to verify the alarm condition; the main control unit is programmable via a keypad; the transceiver communicates at 2.4 GHz; the peripheral units include sensors comprising one or more of door/window sensors, PIR motion sensors, glass break detectors, environmental sensors (temperature sensors, moisture detectors etc.), smoke detectors, combustion gas detectors, carbon monoxide detectors, alarm indicators; and/or each peripheral unit is characterized by a unique preprogrammed ID code.

Brief Description of the Drawings

In drawings which illustrate by way of example only a preferred embodiment of the invention,

Figure 1 is a block diagram illustrating a preferred embodiment of the alarm system of the invention, and

Figure 2 is a perspective view of an optional cordless telephone for the embodiment of Figure 1.

Detailed Description of the Invention

Figure 1 illustrates a preferred embodiment of the security alarm system of the invention. According to the invention, a Main Control Unit (MCU) 20 comprises a wireless transceiver 22 for bi-directional communication with the Peripheral Units 40 including one or more remote sensors 42; digital communicator 24, which controls the data transfer and line seizure functions via telephone link 28, which may be a direct connection to a land line or a wireless connection to a cellular or two-way radio link; a processor 26 for processing communications to and from the Peripheral Units 40 and including a keypad/display driver for processing data input via a built in keypad (not shown) and displaying information on an LCD display (not shown); and an optional home automation link for controlling peripheral devices such as "actuators" (switches or control units), for activating and deactivating appliances, lights etc.

In the preferred embodiment the Main Control Unit 20 communicates with the Peripheral Units 40 via a 2.4 GHz frequency hopping digital spread spectrum RF communications protocol, which is stable over a large distance and resistant to outside interference and ambient noise. Communication preferably occurs at a medium speed (around 115 kbps) through time division multiplexing, however dynamic allocation of the data rate by the MCU 20 allows flexibility when increased throughput or communication reliability is desired for a reduced number of devices. Interference between peripheral signals is prevented by the Main Control Unit 20 which synchronizes peripheral transmissions via the processor 26, whereby the Main Control Unit 20 undertakes a sequential or "cascade" tasking of peripheral sensors 42 and, if status is desired, peripheral alarm indicators 44.

The network topology may be organized in a star configuration, with the MCU 20 as the central entity and the sensors 42 and indicators 44 as the peripheral entities. In addition, a control channel may be provided for network control functions such as standby and controlling, tasking and initializing all Peripheral Units 40.

A higher number of high latency Peripheral Units 40, hundreds in some situations, can be handled by adding collision handling protocols in the application layer. Moreover, used in conjunction with a cordless telephone 10, the cordless telephone handset 12 effectively operates as a Peripheral Unit 40; any number of telephone handsets 12 may be supported by a single telephone 10 used with the invention, and each handset 12 is capable of configuring the alarm system remotely. The system can also be configured by data entered into an external corded or cordless telephone set.

The preferred embodiment of the invention is a 2.4 GHz wireless alarm security system adapted for use with professional monitoring service central station (MSCS), optionally coupled with a fully featured single- or multi-line, single- or multi-handset cordless telephone 10. The invention is designed to be easily and quickly installed, and can be programmed by a person with minimal computer skills using a digital processing device such as a personal computer 38 equipped with suitable software, if necessary with the assistance of the Monitoring Service Operator (MSO) or a Web site featuring instructional information provided by the manufacturer; or optionally by a trained installer using a personal computer 38.

The invention thus comprises a Main Control Unit (MCU) 20 and a plurality of radio frequency (preferably 2.4 GHz) wireless Peripheral Units 40, including peripheral sensors 42 such as wireless security sensor peripheral units (SSPU), wireless environmental sensor peripheral units (ESPU), and wireless actuator peripheral units (APU) 44 such as sirens and strobes. Preferably also the MCU 20 display and keypad provide a means for basic programming and configuration of the system, however as described in greater detail below, in the preferred embodiment all programming and setup of the security alarm system of the invention is advantageously effected through a communications link to a personal computer 38.

In the preferred embodiment the MCU 20 also provides one master access code and nine user programmable access codes; the digital communicator 24 integrated with a two-way modem, for example a 300 baud FSK modem for communication with the MSCS and for remote programming; an optional voice dialer for dialing one or more predetermined telephone numbers to alert the user and/or the MSO of any of a number of predefined conditions according to prerecorded voice messages or alphanumerical codes; a 110 dB siren 43 with user programmable sequences for multiple alarm conditions (for example alarm, panic and life-safety); a power supply with backup battery and trickle charger; a communications port 39 for a PC connection, for example RJ11, USB (universal serial bus), RS232, ethernet, firewire etc., or wireless protocol, for system setup and programming; and optionally an X10 compatibility connection 37 for home automation.

The user control panel may comprise a conventional keypad (not shown), optionally backlit, for dialing and code transmission. The keypad may comprise programmable multi-function keys, which enable response to displayed instructions, as well as special buttons: e.g. home arm, away arm "one touch" arming. The preferred display (not shown) is a backlit, 4x32 alphanumeric and/or graphics LCD which is sufficient to clearly indicate the type of alarm (alarm, panic, and life-safety) upon occurrence, and to provide basic instructions for setup and reconfiguration of major functions Indicators include Power/Battery; OFF (system not working) and otherwise as desired. For example, a combination of red and green LED's can be activated in various permutations of constant or flashing to indicate different conditions (e.g. constant green - power and backup battery OK; flashing green - powered by mains, backup battery low; constant red - powered by backup battery, battery OK; etc.). The user interface on the MCU 20 is thus simple and inexpensive, yet versatile enough to control the major functions and indicators provided by the system.

Two-way digital communication between the MCU 20 and the wireless Peripheral Units 40 provides full control and supervision of the system by the MCU 20 and the MSO. The optional 2.4 GHz cordless telephone 10 may include an expanded keypad 12a with special function buttons 12b and a display 12c for activation, control and supervision of all major system security functions.

The processing platform in the invention preferably features expansion capability for home automation, child monitoring, emergency monitoring, etc. Optional built-in cellular radio or connection to an external cellular phone 17 may be used to provide the primary or a back-up link to the monitoring service central station in case of telephone line failure or sabotage. A real-time clock enables time stamping of all system operations and events, in the preferred embodiment stored in a 50-event log memory.

Wireless Peripheral Units 40 may include sensors 42, for example (without limitation) door/window sensors, PIR motion sensors, glass break detectors, environmental sensors (temperature sensors, moisture detectors etc.), smoke detectors, combustion gas detectors, carbon monoxide detectors; video/audio surveillance devices; alarm indicators 44 such as a siren and/or strobe; and remote controllers 19 such as an emergency (panic) transmitter and/or keychain remote control.

In the preferred embodiment the system of the invention has the capacity for a virtually unlimited number of wireless Peripheral Units 40. Each Peripheral Unit 40 is characterized by its own unique preprogrammed ID code, which is preferably stored in non-volatile memory so that replacing batteries in Peripheral Units 40 will not erase the ID code (or any other preprogrammed parameter). Each Peripheral Unit 40 is equipped with an RF processor comprising a transceiver adapted to transmit a digital RF signal including the characteristic digital ID code which is recognized by the MCU 20.

All peripheral parameters (for example ID code, zone, zone attributes, supervision level etc.) are learned/programmed in the MCU 20 and stored in non-volatile memory. Peripheral parameters can be changed by reprogramming, or can be cleared from the MCU 20 non-volatile memory using a Master Access Code (MAC) and Master Reset Sequence (MRS). The MRS should include audio and/or visual warnings to prevent accidental operation. The MCU 20 may also provide a built-in siren and/or strobe 44, programmable to be activated concurrently with or subsequent to communication of an alarm situation to the MSO. The MCU 20 internal backup battery with trickle charger provides backup operation, including communication with Monitoring Service Central Station, in case of mains power interruption. A low back-up battery alert (and optional alert call to the MSO) is activated before the battery is discharged to a "non-operational" condition.

Zone type definitions are also learned/programmed in the MCU 20 and stored in non-volatile memory, for example (without limitation): entry/exit, instant, interior, delay 1, delay 2, fire (24 hour), burglary (24 hour), emergency (24 hour), additional zones (24 hour) with unique SIA identifiers, additional latchkey zones (24 hour). Current 2.4 GHz technology allows a wireless indoor range between the MCU 20 and Peripheral Units 40 of around 100 meters, which is suitable for most applications.

During operation all peripheral sensors 42 are fully supervised, by the MCU 20 and optionally by the MSO, and report any desired status including (without limitation) Battery Low, Tampering Attempt and Change of Status (open/close for door/window and detection for PIR) to the Main Control Unit 20 and optionally to the MSO, upon occurrence and/or interrogation. The MCU 20 also tracks attempted jamming of communications with supervised Peripheral Units 40 and supervisory failures, and optionally reports to the MSO. The MCU 20's built-in digital communicator 24 supports most major communications formats, enabling two-way communication protocol with the MSCS, for alarm reception, verification and analysis, remote programming, and any other desired functions. Peripheral Units 40 signal a "low battery" alert condition to the MCU 20 (and optionally to the MSO) a preset time interval before full battery discharge.

According to the preferred embodiment of the invention, the MCU 20 can be programmed and configured by:

1. A local computer, for example a personal computer (PC) 38, via a standard RJ11, USB or RS232 connection, or any other suitable wired or wireless connection, in conjunction with MCU programming software;

2. An accessory or built-in modem connection to a remote computer, for example remote uploading/downloading by the MSO from the MSCS; or

3. Data entry through the MCU 20 keypad and display (for basic programming only).

Through the remote connection the MSO can fully control system activation and deactivation, perform system maintenance, upload commands (e.g. "listen in" at high or low

volume), and/or receive reports of situations on the secured premises, thereby enabling an appropriate response.

An optional built-in cellular radio or connection to an external cellular phone 17 or two-way pager (not shown) provides the primary communications link, or a backup communications link, to the MSCS in case of telephone line failure or sabotage by an intruder. The system may also provide a Telephone Line Monitoring (TLM) feature, which checks the state of the telephone line at predetermined intervals, identifies line failure or sabotage, sounds an audio alarm and/or (where a backup line is provided) notifies the MSO via the backup cellular or pager communications link. The cellular phone 17 can also be used instead of a conventional telephone line 28 as the main telephone connection to the MSO, with or without a backup communications link.

The system may communicate on a dedicated telephone line 28, or share a telephone line with other devices. In shared telephone line installations, the system of the invention may be implemented with a line seizure device, for example an RJ-31X/CA-38A box, and the telephone line seizure function will interrupt any telephone call in progress in response to an alarm condition and seize the telephone line to call the MSCS.

The system of the invention may be advantageously used in conjunction with a telephone set, preferably a 2.4 GHz (or other wireless frequency) cordless telephone 10 having a base station 11 and handset 12, which may include an expanded keypad 12a with special function buttons 12b and a display 12c for activation, control and supervision of all major system security functions. This allows for DTMF remote control access of security system, through which selected security features can be activated and deactivated (using appropriate DTMF access codes) from a remote telephone through a connection, for example RS232, between the base station 11 and the MCU 20. A corded telephone may also may also be used for this purpose. In the preferred embodiment the invention is also home automation compatible through X10 port 37, which allows for the timed or remote control of lighting, HVAC etc.

The optional telephone accessory 10 is preferably a cordless single- or multi-line, single- multi-handset instrument. Each cordless telephone handset 12 communicates with the cordless base station 11 by conventional communications protocols, preferably at 2.4 GHz

but optionally at lower frequencies (for example 900 MHz). The cordless handset 12 may be modified to include additional security-related buttons and displays as selected, and preferably provides the following features:

1. A multi-function LCD display 12c, minimum two-line, for displaying information, such as caller ID code, called number, and alarm status and messages;

2. Alarm arming and disarming, whereby the MCU 20 can be programmed for "one touch" arming on the handset 12; and

3. Panic Alarm activation by depressing a preset key or simultaneously depressing a combination of keys, for example the "*" and "#" keys.

Figure 2 illustrates by way of example a cordless telephone 10 which may be used in conjunction with the system of Figure 1, comprising a handset 12 in communication with a base station 11. A keypad 12a is provided for dialing the telephone, and for entering alphanumeric data for programming and setting the alarm system in conjunction with special function buttons 12b. A display 12c, for example an LCD display window, provides user information in both the telephone and alarm system modes.

The default mode of the cordless telephone handset 12 and base station 11 should be telephone mode. When switched to security mode, the telephone 10 will remain in security mode for a preset interval after the last command, then return automatically to telephone status. Upon command, the telephone 10 will switch back to telephone mode without any delay.

In addition to a standard keypad and telephone function buttons, two dedicated security buttons 12b may be provided on the cordless handset 12: A "Select security Mode" button and an "Enter" or "OK" button. A graphic, backlit LCD display 12c may be used to perform the security operational requirements, displaying a selection of 4 to 8 menus with 3 to 4 submenu levels.

In security mode, the cordless handset 12 should be able to transmit strings of at least 8 to 12 digits to the MCU 20 via the cordless base station 11. DTMF coded digits are sufficient for this purpose. Any other format of digital coding may be used. Decoding of the

data sent by the cordless handset 12 is implemented by the MCU 20. In security mode, the cordless handset 12 (or any additional dedicated control unit) reads the sequence of keypad operations, stores it in a buffer and sends it out to the MCU 20 when an "Enter/OK" button 12b is depressed.

A full alphanumeric data transmission is preferred. A full display configuration or setup may require 2,000 to 3,000 bit or 250 to 400 byte capacity. DTMF code is typically too slow for the amount of data required for this function, so another digital coding format may be used. The cordless handset 12 (or additional dedicated control unit) should also be able to receive data sent by the MCU 20 and to display it on the handset display 12c.

The telephone base station 11 serves merely as a transparent repeater (i.e. with no additional information processing) for communication between the cordless handset 12 and the MCU 20. Accordingly, the telephone base station 11 is preferably provided with a communication channel (serial format is preferred) to enable two-way communication. The MCU 20 receives information input by the user via the handset 12, and responds by transmitting to the handset 12 information regarding the display format and content. The MCU 20 is thus connected to the cordless base 11 DTMF generator and display driver.

Another optional accessory for the system of the invention is a keychain-size battery-powered remote control 19 with any desired number of control buttons, which enable remote arming/disarming of the security system. Each remote control unit 19 is characterized by a unique factory-programmed ID code, which is used for the home monitoring feature. A 2.4 GHz transceiver allows for both remote control of system functions and remote monitoring of status, including alarm and low battery indications.

To install the system of the invention, the installer selects a location for the Main Control Unit 20 and connects it to mains power supply (through an appropriate standard low-voltage power adapter, preferably with an approved AC isolation transformer). The installer determines the location of each Peripheral Unit 40 and installs the Peripheral Units 40 in the selected locations. The installer connects a digital processing device, for example a personal computer (PC) 38, to the communications port 39 provided in the MCU 20 (or in the case of a wireless connection, sets up the PC 38 within range of the communications port 39), and activates the programming software, which may be contained on a CD ROM or other media

packaged with the system. The setup software initiates and checks communication with the Main Control Unit 20, and through a series of menus and/or other user interfaces, the setup software guides the installer to enter the Master Access Code (a default Master Access Code is supplied with the system) in order to initiate system installation and programming.

The setup software guides the installer to enter the other lower level access codes and all programmable Main Control Unit 20 parameters (e.g. exit/entry time delays, etc.) or to specify the use of default settings. The setup software guides the installer to enter the locations of the Peripheral Units 40 and each Peripheral Unit's setup parameters including zone type (e.g. Entry/Exit, Instant, Interior, Delay 1, Delay 2, Fire (24 hour), Burglary (24 hour), Emergency (24 hour), Additional Zones (24 hour) with unique SIA identifiers, Additional Latchkey Zones (24 hour) etc.) and zone attribute (Audible/Silent, Chime, bypass, latchkey etc.), and to activate each of the Peripheral Units 40 (for example by inserting the battery) at a point where the MCU 20 is enabled to receive the ID code of the Peripheral Unit 40, so that the MCU 20 can "learn" the ID code of each Peripheral Unit 40. The installer may also setup user-programmable access code attribute (e.g. zone bypass, duress, guest one-time code).

The setup software guides the installer to connect the Main Control Unit 20 to the telephone line 28. If the required Line Seizure hardware is installed, the setup software guides the installer to enable this feature. The installer tests the system installation in test mode, and may register the system by calling a prearranged Monitoring Service Operator. The MSO, in turn, contacts the MCU 20 to verify correct installation, make any necessary programming changes and activate the system in fully operational mode.

Thereafter the system can be programmed on-site by the installer, by means of an on-site PC 38 and cable (or wireless) connection; or remotely by the Monitoring Service Operator from the MSCS or other remote location, by means of a remote PC (not shown) and a modem. Limited on-site programming is available directly from Main Control Unit keypad and display, according to the system manual. All functions programmable through the Main Control Unit keypad and display can also be programmed via upload/download.

In operation, the system is armed by:

1. "Away" arming, all interior zones and perimeter zones active, by entering the access code, pressing the "Away" arming button and exiting premises through a designated door;

2. "Home" arming, only perimeter zones active, by entering the access code and pressing the "Home" arming button without exiting the premises.

3. Bypass arming (Home or Away) via the MCU 20 keypad, enabling arming with bypass of selected interior and/or perimeter zones, by entering the access code followed by bypass codes for the sensor(s) 42 to be bypassed and then pressing the "Home" or "Away" arming button.

4. Auto arming via the MCU keypad, with auto bypass, enables programming the system to arm itself at a predetermined time, automatically bypassing any zones not ready for arming at that time.

The system will thereafter sound an alarm condition if any of the sensors 42 are tripped or the "Panic" button is depressed on any remote device. The alarm may be silent or audible, depending on the programming, and initiates a blinking message on the MCU display identifying the type of alarm, and optionally a report to the Monitoring Service Operator. In embodiments of the system which are not monitored, the alarm would be audible and a voice dialer or DTMF dialer could be employed to send a pre-recorded message or code to one or more pre-programmed telephone numbers stored in the MCU 20 memory.

The "Panic" mode initiates an alarm condition whether or not the system is armed, and preferably can be activated by pressing a "Panic" button on the MCU 20, by pressing the "Panic" button on the Keychain Remote Control 19, or by pressing a selected combination of keys (for example "*" and "#") on the optional cordless telephone handset 12.

To reduce opportunities for false alarms, the system provides an audible exit delay and audible exit fault signal when the system is "Away" armed. Preferably, when the system is "Away" armed detection of motion within the premises without detection of a perimeter

violation will initially activate the local siren 44 only, and will alert the MSO only after a preset interval. Likewise, when the system is "Home" armed a perimeter violation will initially activate the local siren 44 only, and will alert the MSO only after a preset interval.

A security sensor or an environmental sensor (for example a temperature or humidity sensor) indicates an alarm condition by transmitting its characteristic RF signal to the Main Control Unit 20. In the preferred embodiment the MCU 20 then sends a signal to the sensor 42 requesting a status signal from the sensor 42, to verify the alarm condition. The main control unit 20 may also, or alternatively, request a status signal from a neighboring sensor 42 (for example a motion detector in the vicinity of a door contact that goes into an alarm condition). If the activated sensor 42 and/or the neighboring sensor 42 indicates in response to the verification request that no alarm condition exists, the main control unit 20 determines whether the alarm indication was false according to parameters programmed into the MCU 20. This can reduce the likelihood of false alarms to produce a more reliable alarm system.

Moreover, the verification request signal transmitted by the main control unit 20 can be an 'acknowledgment' to the sensor 42 that its signal disruption has been logged by the Main Control Unit 20, failing which after a predetermined interval the sensor 42 may transmit another signal to the main control unit 20 requesting an acknowledgment signal.

In either case the main control unit 20 or the sensor 42 preferably continue to transmit requests for sensor status or acknowledgment until a response signal is received. Thus, the two-way communication between the Main Control Unit 20 and the sensors 42 provide a "smart" system which can verify indications and system conditions before communicating with a monitoring station or activating an alarm indicator 44.

The system of the invention preferably attempts to call the Monitoring Service Operator in order to report security status when any valid reporting event occurs. The system may be programmed to use DTMF or pulse dialing, and contacts the MSO via the MSO's programmed telephone number (or numbers if more than one is available). The system will continue dialing the preset number of times until the MSO answers with the appropriate handshaking procedure.

Once contact with the MSO is established, the appropriate reporting format (programmed when the system is installed) is initiated. The digital communicator 24 in the MCU 20 supports all major communication reporting formats. As recommended by the Security Industry Association (SIA) in its study of data formats (October 1997), the system preferably uses half-duplex asynchronous FSK modulation, operating at 300 baud, with a single modem serving both for communication with the MSO and for remote programming. This standard enables a wide variety of options and information transmission, and is likely to be adopted by most, if not all, MSO's. In an alarm mode the MCU 20 sends a code to the MSO indicating the event that occurred, time stamped by the real-time clock integrated into the MCU 20, enabling the MSO to provide an appropriate response.

As noted above, in embodiments of the system which are not monitored, the built in voice dialer or DTMF dialer could be employed to send a pre-recorded message or code to one or more pre-programmed telephone numbers stored in the MCU 20 memory to contact, for example, a cellular telephone or pager carried by a homeowner, security manager etc.

The device preferably operates in three modes: Active Mode, in which data is actively being transferred between the MCU 20 and Peripheral Units 40; etc.; Standby Mode, in which the Peripheral Units 40 are communicating with the MCU 20 periodically solely for maintaining network synchronization and control; and Suspend Mode, in which selected Peripheral Units 40 are not communicating with the network. A 'wakeup' signal from the MCU 20 is required to restore communication with the MCU 20. This mode is ideal for power conservation and selective zone control and deactivation.

The Peripheral Units 40 may also include a microphone/speaker (not shown) for two-way voice communication within or about the premises and for "listening in" by the MSO; any number and variety of sensors 42; one or more wired or wireless video cameras (not shown) for communicating a video surveillance signal to the MCU 20 which can be accessed remotely through the communications link; and/or one or more alarm indicators 44.

The Peripheral Units 40 can be reconfigured, added and removed from the system as needed. For example, in preparation for an off-hours delivery a sensor 42 on the shipping door and a neighboring motion detector can be deactivated, leaving all other sensors 42 active. The system may also activate an actuator controlling the shipping door lock, allowing

delivery personnel access to the premises. In this fashion each particular sensor 42, actuator 19 and alarm indicator 44 can be considered to constitute a "zone". This function should preferably be configurable from the MCU keypad.

The main control unit 20 can also be programmed to associate specified groups of peripherals 40 as separate zones, for ease of activating/deactivating portions of the system. These groups can be reconfigured on site or remotely, as desired.

It is also possible using the system of the invention to transmit from, for example a sound detector, rather than simply an indication that sensor 42 has detected a sound, a digital representation of the sound level. Thus, the Main Control Unit 20 can be programmed to ignore sound levels below a certain threshold, to account for ambient noise levels. The threshold can change by a preprogrammed schedule, for example a lower threshold indicates an alarm condition at night, and the threshold can be changed remotely or on site as desired.

Troublesome zones can be repaired or isolated from the system. For example, a vibration sensor 42 that activates persistently over a predetermined interval can be reconfigured, or the Main Control Unit 20 can discriminate from other Peripheral Units 40 by, for example, not communicating with the monitoring service when the troublesome sensor indicates an alarm condition, but still indicating the alarm condition locally by an alarm indicator 44 and/or in the Main Control Unit 20's event log, or by auto-dialing one or more stored telephone/pager numbers and playing a pre-recorded message or sending a preset code.

In the case of a monitored system, the Monitoring Service Operator can configure the Main Control Unit 20 to limit the ability of the occupier of the premises to configure certain Peripheral Units or perform other procedures. In the case of a homeowner installed system, the system can be programmed to remain inactive until an MSO conducts a diagnostic to confirm that the Main Control Unit 20 and all Peripheral Units 40 are operating properly.

Monitoring of so-called "latchkey children" is facilitated by the invention. Preprogrammed arrival times can be selected for one or more children, and the auto-dial or alarm functions can be initiated automatically if a child has not disarmed the system by the arrival time. The child can alternatively wear a sensor 42, which will be detected by the

system upon arrival of the child, if desired disarming a designated entry point. These parameters can be reconfigured remotely by the homeowner if circumstances so dictate.

Connection of the system to a personal computer enables Internet access and other on-line functions and capabilities, if desired. This can offer an alternative to telephone, PCS etc. for remote management of the system.

The following standards may be relevant to the above description and are incorporated herein by reference:

US Standards

1. CFR 47, Part 15 (FCC).
2. CFR 68.
3. SIA Audio Verification Standards.
4. SIA Control Panel Standards.
5. UL-609 Local Burglar Alarm Units and Systems.
6. UL-639 Intrusion Detection Units.
7. UL-1023 Burglar Alarm System Unit, Household
8. UL-1610 Central Station Burglar Alarm Systems.
9. UL-1635 Digital Burglar Alarm.
10. UL-1641 Installation and Classification of Residential Burglar Alarm Systems.

Canadian Standards

1. ULC-5306 Standard for Intrusion Detection Units.

EEC Standards

1. CEPT/ERC/REC 70-03E.

2. EN 300-220 Radio Equipment and Systems; Short Range Devices Operating in the 25 MHz - 1 GHz Range with Power Level up to 500 MW.

3. EN 41003 Electrical Safety Standards.

4. EN 50081 and EN 50082 Electromagnetic Compatibility.

5. EN 50111-3-1 Alarm Systems In and Around Buildings.

6. EN 50131-2-2 Alarm System - Intrusion System.

7. EN 55011 Limits and Methods of Measurement of Radio Disturbance Characteristic of Industrial, Scientific and Medical RF Equipment.

8. EN 60950 Safety of Information Technology Equipment Including Electrical Business Equipment.

A preferred embodiment of the invention having been thus described by way of example, it will be appreciated by those skilled in the art that certain adaptations and modifications may be made without departing from the scope of the invention. The invention is intended to include all such variations and modifications as fall within the scope of the claims.

WE CLAIM:

1. A security alarm system, comprising

one or more peripheral units, and

a main control unit comprising an RF transceiver for communicating with the one or more peripheral units, whereby the main control unit receives a signal from the one or more peripheral units to indicate an alarm condition, and a digital communications port,

wherein the main control unit can be connected to a digital processing device through the digital communications port, whereby data entered into the digital processing device programs the main control unit.

2. The security alarm system of claim 1 wherein the main control unit communicates data to the one or more peripheral devices to configure and control said peripheral devices.

3. The security alarm system of claim 1 wherein the main control unit comprises a communicator for controlling a transfer of data between the system and a remote location over a communications link.

4. The security alarm system of claim 1 wherein a keypad or a display, or both, for entering information into and displaying information from the main control unit are contained in a remote unit comprising a cordless telephone handset.

5. The security alarm system of claim 1 wherein in response to an indication of an alarm condition by a sensor, the main control unit requests a status signal from the sensor to verify the alarm condition.

6. The security alarm system of claim 1 wherein in response to an indication of an alarm condition by a sensor, the main control unit processes a status signal from one or more neighboring sensors to verify the alarm condition.

7. The security alarm system of claim 1 wherein the main control unit is programmable via a keypad built into the main control unit.

8. The security alarm system of claim 1 wherein the transceiver communicates at 2.4 GHz.

9. The security alarm system of claim 1 wherein the peripheral units include sensors comprising one or more of door/window sensors, PIR motion sensors, glass break detectors, environmental sensors (temperature sensors, moisture detectors etc.), smoke detectors, combustion gas detectors, carbon monoxide detectors, alarm indicators

10 The security alarm system of claim 9 wherein each peripheral unit is characterized by a unique preprogrammed ID code.

11. A method of programming a security alarm system comprising one or more peripheral units and a main control unit comprising an RF transceiver for communicating with the one or more peripheral units, whereby the main control unit receives data from the one or more peripheral units to indicate an alarm condition, and a digital communications port, comprising the steps of

a. connecting the main control unit to a digital processing device through the digital communications port, and

b. entering data into the digital processing device to program the main control unit.

12. The method of claim 11 including the step of communicating data from the main control unit to the one or more peripheral devices to configure and control said peripheral devices.

13. The method of claim 11 including the step of controlling a transfer of data between the system and a remote location over a communications link.

14. The method of claim 11 wherein a keypad or a display, or both, for entering information into and displaying information from the main control unit are contained in a remote unit comprising a cordless telephone handset.

15. The method of claim 11 including the step of, in response to an indication of an alarm condition by a sensor, requesting a status signal from the sensor to verify the alarm condition.

16. The method of claim 11 including the step of, in response to an indication of an alarm condition by a sensor, processing a status signal from one or more neighboring sensors to verify the alarm condition.

17. The method of claim 11 wherein the main control unit is programmable via a keypad built into the main control unit.

18. The method of claim 11 wherein the wireless transceiver communicates at 2.4 GHz.

19. The method of claim 11 wherein peripheral units include sensors comprising one or more of door/window sensors, PIR motion sensors, glass break detectors, environmental sensors (temperature sensors, moisture detectors etc.), smoke detectors, combustion gas detectors, carbon monoxide detectors, alarm indicators.

20. The method of claim 11 wherein each peripheral unit is characterized by a unique preprogrammed ID code.

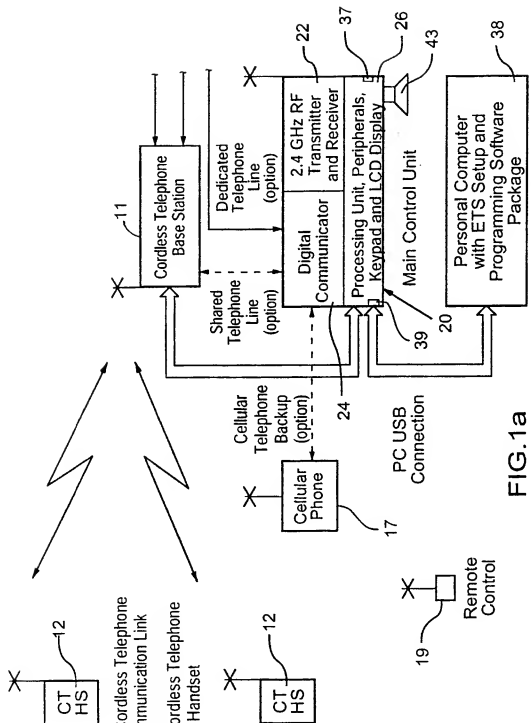

CT HS
12
CT HS
12
2.4 GHz Cordless Telephone RF Communication Link
CTHS=Cordless Telephone Handset
19
Remote Control
Cellular Phone
17
Cellular Telephone Backup (option)
24
PC USB Connection
Cordless Telephone Base Station
11
Shared Telephone Line (option)
Dedicated Telephone Line (option)
Digital Communicator
2.4 GHz RF Transmitter and Receiver
22
Processing Unit, Peripherals, Keypad and LCD Display
37
Main Control Unit
26
43
39
20
Personal Computer with ETS Setup and Programming Software Package
38

FIG.1a

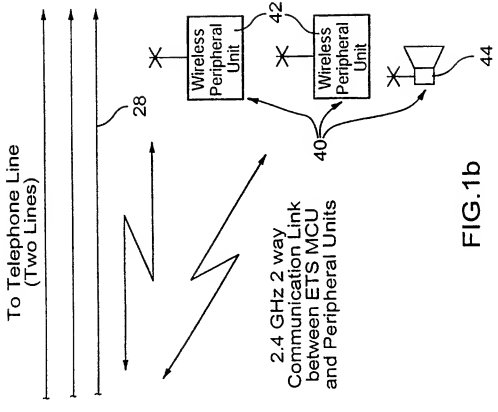

To Telephone Line
(Two Lines)
28
Wireless Peripheral Unit
42
Wireless Peripheral Unit
40
44
2.4 GHz 2 way Communication Link between ETS MCU and Peripheral Units

FIG. 1b

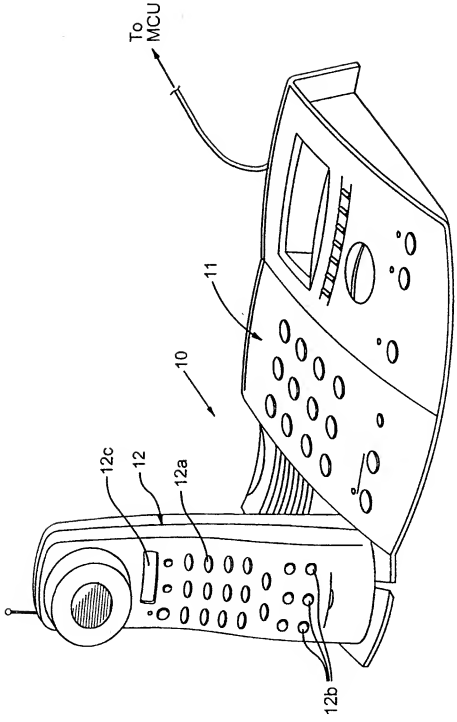


FIG.2

INTERNATIONAL SEARCH REPORT

Internat ·l Application No
PCT/CA 00/00662

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G08B25/14 G08B26/00 G08B25/10 G08B25/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G08B H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, PAJ, EPO-Internal, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"WLS900 Marquis Wireless. Technical specifications." 'Online! February 1999 (1999-02) , DIGITAL SECURITY CONTROL , ONTARIO, CANADA XP002150081 Retrieved from the Internet: <URL: www.dsc.com> 'retrieved on 2000-10-13!	1,3, 9-11,13, 19,20
Y	the whole document	7,8,17, 18
A		5,6,15, 16
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 October 2000	30/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx 31 651 epo nl, Fax: (+31–70) 340–3016	De la Cruz Valera, D

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna nl Application No
PCT/CA 00/00662

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No
Y	"LMX3162 Enabling 2.4GHz applications" 'Online! 23 February 1999 (1999-02-23) , NATIONAL SEMICONDUCTOR , USA XP002150082 Retrieved from the Internet: <URL: http://www2.national.com/appinfo/wireless/tech/ismtech.pdf > 'retrieved on 2000-10-13! page 3 page 10 ---	8,18
Y	WO 98 49663 A (DIGITAL SECURITY CONTROLS LTD ;PETERSON JOHN (CA); PARKER JAMES (C) 5 November 1998 (1998-11-05) figure 2 ---	7,17
A	PATENT ABSTRACTS OF JAPAN vol. 017, no. 421 (E-1409), 5 August 1993 (1993-08-05) & JP 05 083412 A (TOKYO GAS CO LTD), 2 April 1993 (1993-04-02) abstract ---	4,14
A	US 4 772 876 A (LAUD TIMOTHY G) 20 September 1988 (1988-09-20) column 4, line 38 - line 51 column 5, line 35 - line 50 claim 1 ---	1,2,11
A	US 4 581 606 A (MALLORY JOHN) 8 April 1986 (1986-04-08) the whole document ---	1,11
P,X A	WO 99 35623 A (PITTWAY CORP) 15 July 1999 (1999-07-15) page 1 page 15, line 7 - line 32 -----	1,7,11, 17 2-6, 8-10, 12-16, 18-20

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna l Application No
PCT/CA 00/00662

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9849663 A	05-11-1998	CA 2203591 A EP 0978111 A	24-10-1998 09-02-2000
JP 05083412 A	02-04-1993	NONE	
US 4772876 A	20-09-1988	NONE	
US 4581606 A	08-04-1986	NONE	
WO 9935623 A	15-07-1999	AU 2029199 A	26-07-1999